(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2000－276330
（P2000－276330A）
(43)公開日　平成12年10月６日(2000.10.6)

(51)Int.Cl.'	識別記号	ＦＩ		テーマコード'(参考)
Ｇ０６Ｆ　7/58		Ｇ０６Ｆ　7/58	Ａ	５Ｊ１０４
Ｇ０９Ｃ　1/00	６５０	Ｇ０９Ｃ　1/00	６５０Ｂ	

審査請求　未請求　請求項の数８　ＯＬ　（全５頁）

(21)出願番号　特願平11－82973

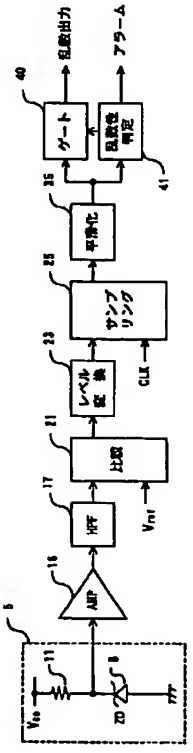
(22)出願日　平成11年３月26日(1999.3.26)

(71)出願人　596131492
システム工学株式会社
東京都千代田区神田錦町１－15－11
(71)出願人　599041020
吉田　隆一
福岡県飯塚市川津680－４
(72)発明者　長井　剛一郎
神奈川県川崎市宮前区馬絹858番地　カサベルデ宮崎台505号
(72)発明者　吉田　隆一
福岡県飯塚市川津680－４
(74)代理人　100079119
弁理士　藤村　元彦

Ｆターム(参考)　5J104 AA27 FA10

(54)【発明の名称】　故障判断機能を備えた乱数生成装置

(57)【要約】
【目的】　自身の故障を判別して、非真正な乱数出力の出力を防止する。
【解決手段】　乱数生成部から得られる乱数データを取り込んで取り込んだ乱数データの乱数性を検定して、乱数性が不十分であることを判定したときには、乱数データの出力を禁止する。



1

【特許請求の範囲】

【請求項１】　物理乱数データを生成する乱数生成手段と、前記物理乱数データを取り込んで取り込んだ物理乱数データの乱数性が不十分である場合、前記物理乱数データの次段への出力を禁止する禁止手段と、からなることを特徴とする乱数生成装置。

【請求項２】　前記禁止手段は、前記物理乱数データの内の同一データ値の出現確率に基づいて、前記物理乱数データの乱数性を判定することを特徴とする請求項１記載の乱数生成装置。

【請求項３】　前記禁止手段は、前記物理乱数データの内の同一データ値の出現確率の一様性、非周期性、非系列性、の順に検定することを特徴とする請求項２記載の乱数生成装置。

【請求項４】　前記乱数生成手段は、接合を含む半導体素子と、降伏電流が生じる程の逆バイアス電圧を前記接合に印加する逆バイアス印加手段と、前記接合を含む電流路に生ずる雑音信号をサンプリングして得られるデジタル信号を乱数として出力するデジタル化回路と、からなることを特徴とする請求項１記載の乱数生成装置。

【請求項５】　前記雑音信号の増幅信号を得る増幅回路と、

前記増幅信号を所定の基準電圧と比較して２値化信号を得る比較回路と、

前記２値化信号をサンプリングして、０及び１からなるサンプリング値系列を得るサンプリング回路と、を有することを特徴とする請求項４記載の乱数生成装置。

【請求項６】　前記半導体素子は、ツェナーダイオードであることを特徴とする請求項４又は５記載の乱数生成装置。

【請求項７】　前記サンプリング値系列における０及び１の各々の発生確率が略等しくなるように前記基準電圧を制御する制御手段を有することを特徴とする請求項５記載の乱数生成装置。

【請求項８】　前記サンプリング値系列における０及び１の発生確率が略等しくなるように前記サンプリング値系列を平滑化する手段を有することを特徴とする請求項５記載の乱数生成装置。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】本発明は、乱数生成装置に関する。

【０００２】

【関連技術】本願出願人は、物理乱数を用いた乱数生成装置を開発し、これを特願平１０－２３２８２３号において開示した。かかる乱数生成装置から得られる乱数を用いて、文書管理の識別のためのキーワードとする装置も考えられ、本出願人は、かかる装置についても、特願平１１－４６０８５号において開示した。

【０００３】このような装置において、万一、物理乱数

2

を生成する半導体素子の劣化や関連回路の断線のような故障が発生して、乱数生成装置が真正乱数データを出力しない場合、文書管理装置が正しく動作せず、必要な文書が読み出せないということになり、重大な問題を引き起こすおそれがある。

【０００４】

【発明が解決しようとする課題】本発明は、かかる問題に対処すべくなされたものであり、自身の故障を検知して対処し得る乱数生成装置を提供することを目的とする。

【０００５】

【課題を解決するための手段】本発明による乱数生成装置は、自身の生成する乱数データを一旦取り込んで記憶して、取り込んだ乱数データの乱数性を確認し、取り込んだ乱数データの乱数性が不十分であると判断した場合、乱数データ出力を停止するようになっている。

【０００６】

【発明の実施の形態】以下、本発明の実施例を図面を参照しつつ詳細に説明する。図１は、本発明による第１の実施例である乱数生成装置の構成を示している。また、図２は図１に示した乱数生成装置の動作を説明する図であり、主要な回路ブロックの出力信号を示している。

【０００７】図１において、５は雑音発生回路である。ツェナーダイオード８のｐｎ接合に抵抗器１１を介して降伏が生じる程度の逆バイアス電圧を印加している。これにより、逆方向に微弱な降伏電流が流れ、ランダムな雑音電圧が発生する。このようにツェナーダイオード８を動作させることにより、ツェナ電圧を中心とした、ピークートゥーピーク（peak-to-peak）で数十～数百μＶ程度のランダムな雑音電圧出力が得られ、これを乱数の発生源としている。

【０００８】具体的には、電源電圧Ｖｃｃを＋１２Ｖとし、ツェナーダイオード８にはツェナ電圧が６．３Ｖと電源電圧の約１／２であるものを用いた。ツェナーダイオード８には５６０ｋΩの抵抗器１１を介して逆バイアス電圧を印加することにより、約１０μＡの逆方向電流が流れ、６．３Ｖを中心にpeak-to-peak電圧が約２００μＶ、平均周波数が６０～７０ｋＨｚ程度の雑音電圧が発生する。（図２（ａ）参照）

雑音発生回路５で得られた雑音電圧は微弱であるので、これを増幅回路１５を用いて電圧増幅する。具体的には、２段のオペアンプを用いている。この増幅回路１５の電圧利得は約７４ｄＢで、６．３Ｖを中心としたpeak-to-peak電圧が１Ｖ程度の増幅出力を得ることができる。（図２（ｂ）参照）

次に、増幅回路１５により増幅された雑音出力は、ハイパスフィルタ１７に供給され低周波成分が除去される。ハイパスフィルタ１７のカットオフ周波数は、後述するサンプリングの周波数の２倍程度であればよい。ハイパスフィルタ１７の出力は、比較回路２１に供給され、所

定の基準電圧を閾値としてハイレベル、ローレベルに分けられ２値化される。

【０００９】増幅雑音出力は、接地電圧を中心にほぼ対称であるので、接地電圧を基準電圧として増幅雑音電圧の２値化を行うことができる。本実施例においては、基準電圧として非常に安定している接地電圧を用いている。すなわち、結合コンデンサ１９を用い、増幅雑音出力の直流成分をカットした交流成分を比較回路２１に入力している（図２（ｃ）参照）。これにより、接地電圧（０Ｖ）を閾値とした２値化を行うことができる。この構成においては、温度変化によってツェナ電圧が変化しても、直流成分が増減するのみで２値化には全く影響は生じない。従って、比較回路２１の入力端には０Ｖを中心にしたpeak-to-peak電圧が１Ｖ程度の増幅雑音電圧の交流成分が入力され、接地電圧である０Ｖを閾値とした２値化が行われる。

【００１０】比較回路２１の出力は、レベル変換回路２３に入力され、後段のサンプリング回路２５の論理電圧レベルに変換される。レベル変換回路２３の出力は、周期性のないランダムな矩形波である（図２（ｄ）参照）。この矩形波は、サンプリング回路２５に供給される。サンプリング回路２５は、入力矩形波の周波数に対してある程度低い（数分の１程度以下の）一定周波数で入力矩形波のサンプリングを行い、０及び１のビットからなる系列を得る。入力矩形波には周期性がなく、またサンプリングのタイミングは入力矩形波の周波数とは独立であるので、得られたビット系列は、０，１の各々の発生確率が等しければ、真正乱数系列であることが期待できる。

【００１１】また、サンプリング回路２５において得られた乱数系列の０及び１の各々の発生確率が等しくなるように平滑化処理をなす平滑化回路３５をサンプリング回路２５の後段に設けている。平滑化は、インバランスな０，１の系列を、x_1，x_2，x_3，…とし、得られる乱数をｙとしたとき、

【００１２】

【数１】

$$y = x_1 \oplus x_2 \oplus \cdots \oplus x_n$$

を用いて行うことができる。ここで、

【００１３】

【外１】

$\oplus$

は２を法とする和（排他的論理和）を表す演算である。これにより得られるｙの系列はバランス性が改善されることが示される。すなわち、x_1，x_2，x_3，…の系列中の０の発生確率をｐ，１の発生確率をｑ＝１－ｐとし、ｙに関して０の出現確率をＰ，１の出現確率をＱ＝１－Ｐとすると、ｙのインバランスは、

Ｐ－Ｑ＝（ｐ－ｑ）^{n}

で与えられる。ここで、ｎは平滑化におけるブロックサイズである。ｎを大きくとれば、インバランス性は指数関数的に小さくなる。

【００１４】サンプリング回路２５において得られた０，１からなる真正乱数の系列は、外部インタフェース（図示していない）、例えばＲＳ－２３２Ｃインタフェースなどを介して外部機器へ供給される。尚、サンプリング周波数は、外部機器が必要とするビットレートに設定する必要がある。次に、平滑化回路３５の出力端は、ゲート回路４０及び乱数性判定回路に接続されている。ゲート回路４０は、乱数性判定回路４１からゲートオン指令を受けている限り、平滑化回路３５からの乱数出力を外部出力端子（図示せず）に中継する。そして、乱数性判定回路４１からゲートオフ指令を受けると、乱数出力の中継を停止して、乱数データの外部への出力を停止する。乱数性判定回路は、平滑化回路３５からの乱数データの乱数性を判定して、該乱数データが、十分なる乱数性を備えていることを判定した場合、乱数データの出力を可として、ゲート回路４０にゲートオン指令を供給する。

【００１５】次に、図３のフローチャートを参照しつつ、乱数性判定回路について説明する。　乱数性判定回路４１は、平滑化回路３５からの乱数データ出力が、十分なる乱数性を備えているのかどうかを判定して、もし乱数データが十分なる乱数性を備えている限りゲートオン指令を出力し、該乱数データが十分なる乱数性を備えていないと判断したときにはゲートオフ指令を発するのである。乱数性判定回路４１は、例えば、マイクロプロセッサ（図示せず）によって、形成され、図３に示したフローチャートによって表された乱数性判別サブルーチンを実行することによって、かかる機能を達成する。

【００１６】即ち、このサブルーチンは、例えば、マイクロプロセッサのクロックによって周期的に実行されるメインルーチン（図示せず）によって、適当なタイミングにて割り込んで実行される。このサブルーチンにおいては、先ず、平滑化回路３５から発せられる乱数データｍ（ｍは自然数）ビット分を、順次、取り込んで、所定のメモリに書き込む（ステップＳ１）。そして、書き込まれたｍビットの乱数データの出現頻度を求める。そして、乱数データの出現頻度が一定の範囲において一様に分布しているや否やを例えば、X^2検定を行うことにより、確認する（ステップＳ２）。もし、かかる出現頻度の一様性が確認出来なかったときは、乱数データが乱数性を欠くものであるとして上記したゲートオフ出力を指令する（ステップＳ３）。そして、ブザー音等を発して、アラーム出力をなす（ステップＳ４）。

【００１７】ステップＳ２において、ｍビットの乱数データの出現頻度が一様であると判定した場合、次のステップＳ５において、同一の値の乱数データが周期的に発

生して、取り込んだ乱数データが、非周期性を備えているや否やを例えばX^2検定により確認する。そして、取り込んだ乱数データが、非周期性を充足していないと判断した場合、ゲートオフ出力及びアラーム出力を指令するステップＳ３及びＳ４を実行する。ステップＳ５において、取り込んだ乱数データが非周期性を充足していると判断した場合、次のステップＳ６を実行する。

【００１８】このステップＳ６においては、取り込んだｍビットの乱数データの内、同一データの２次元的出現確率を検定する。そして、この２次元的出現確率の分布が非系列的な分布をしているや否やを確認する。換言すれば、取り込んだ乱数データが非系列的であるということは、１の乱数データから次の乱数データが予測困難であるということである。

【００１９】ステップＳ６において、取り込んだ乱数データの非系列性が確認できなかった場合、ステップＳ３及びＳ４を実行する。一方、取り込んだ乱数データの非系列性が確認された場合、ステップＳ７を実行してゲートオン出力をゲート回路４０に供給する。以上説明した乱数性判別ルーチンにおいては、乱数性の要件として、一様性、非周期性、非系列性の３つの要件を検定しているが、一様性が、最も重要であり、一様性を備えていれば、乱数性を備えていると判断することとしても、実用上問題ない場合も考えられる。

【００２０】また、ステップＳ４のアラーム出力において、一様性、非周期性、非系列性のいずれの要件を欠いているのかを表示して故障修理の便に供することも出来る。なんとなれば、「一様性」欠如の場合は物理乱数発生器の部品の故障による特定の信号（値）の発生、あるいは乱数を暗号システムの暗号鍵に使用した場合に、暗号鍵の統計的予想に基づく暗号解読攻撃の事態が推測出来る。また、「非同期性」欠如の場合は、物理乱数発生器の部品の故障による特定の信号（値）の周期的発生、物理乱数発生装置の乱数発生源であるノイズに装置内部もしくは外部からクロックなどの周期的なノイズが付加される事、あるいは乱数を暗号システムの暗号鍵に使用した場合に、暗号鍵の統計的予想もしくは周期的予想に基づく攻撃の事態が推測出来る。また、「非系列性」欠如の場合は、物理乱数発生器の部品の故障による連続した特定の信号（値）の発生あるいは、乱数を暗号システムの暗号鍵に使用した場合、古い暗号文分析により、暗号鍵を予測する暗号解読攻撃の事態が推測出来るからである。

【００２１】尚、図１においては平滑化回路３５をハードウエアの構成として説明したが、実際はコンピュータのソフトウエアで容易に実現可能であり、コンピュータ側で必要な程度（ブロックの大きさ）で行えば十分である。以上の処理を行うことによって、より真正乱数に近い０，１の系列を得ることができる。そして、平滑化回路３５、乱数性判定回路４１の機能を１つのマイクロコンピュータによって実行することも出来るのである。

【００２２】尚、上記実施例においては、雑音発生源としてツェナーダイオードを用いた場合を例に説明したが、これに限らず、例えば異種導電型の半導体接合を用い、その降伏電流を雑音発生源として用いてもよい。更に、ゲート４０は、例えばＲＳ－２３２Ｃインターフェースの如きいわゆる外部インターフェース回路によって構成することが出来、この場合、ゲートオフ指令は、ＤＴＲ（Data Terminal Ready)をオフにするが如き、いわゆるディスエーブル信号に等価である。

【００２３】

【発明の効果】以上説明したことからも明らかな如く、本発明による乱数生成装置においては、乱数データ出力が、十分なる乱数性を備えているや否やを常時監視して、乱数性を充足していないことを判定した場合、乱数データ出力を停止することとしているので、万一、乱数生成装置が故障しても、乱数データに基づいて動作する文書管理装置等が不適切な動作をすることを防止できる。

【００２４】従って、本装置を、例えばパーソナルコンピュータ等に「真性乱数発生エンジン」として組み込むことにより、デジタル署名アルゴリズムを用いた署名生成のための「真性乱数（物理乱数）」を提供することができると共に、すなわち、従来用いられてきた擬似乱数を用いた場合に比べはるかにセキュリティ確度の高い通信を行うことが可能となる。

【図面の簡単な説明】

【図１】本発明による乱数生成装置を示すブロック図である。

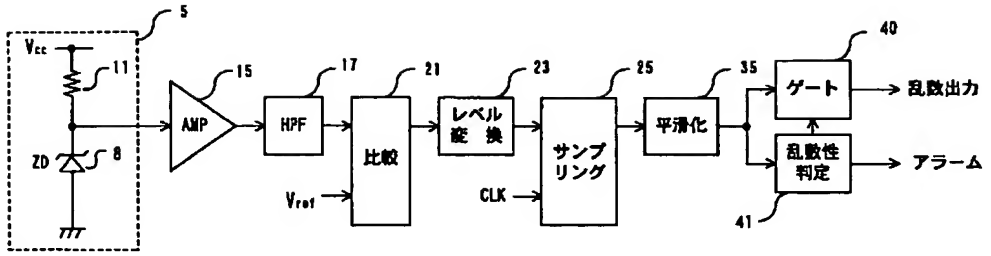
【図２】図１に示された乱数生成装置の乱数生成動作を説明する波形図である。

【図３】図１に示された乱数生成装置の乱数性検定動作の例を示すフローチャートである。

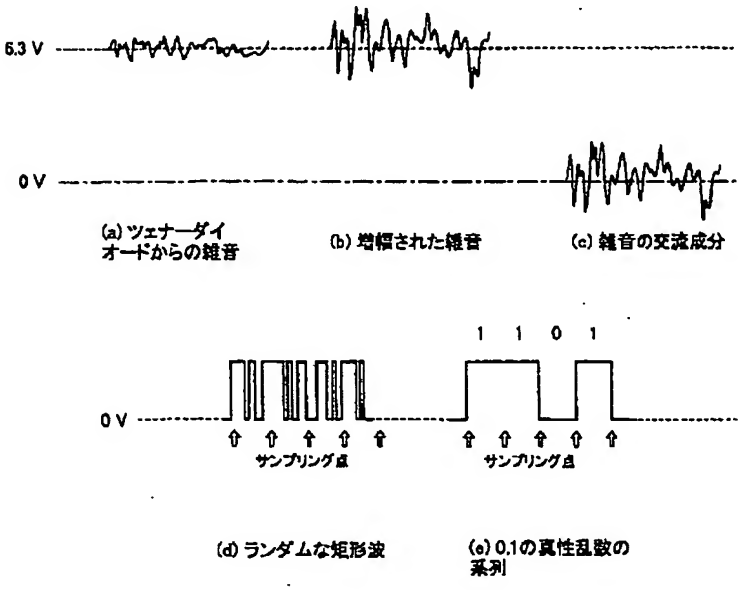
【主要部分の符号の説明】

５　雑音発生回路
８　ツェナーダイオード
１７　ハイパスフィルタ
２１　比較回路
２３　レベル変換回路
２５　サンプリング回路
３５　平滑化回路
４０　ゲート回路
４１　乱数性判定回路

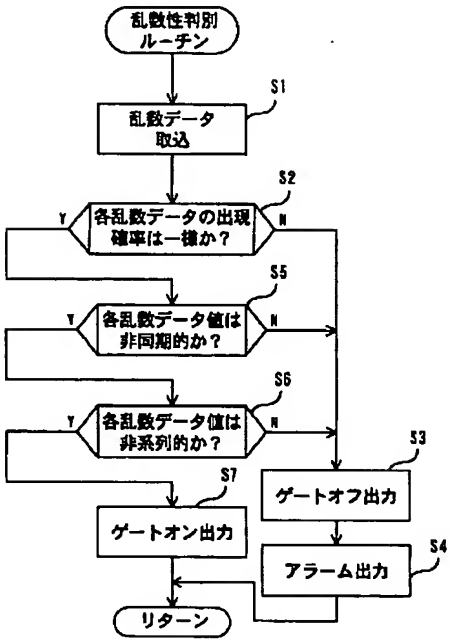
【図１】


5
Vcc
11
ZD
8
AMP
15
HPF
17
Vref
比較
21
レベル変換
23
CLK
サンプリング
25
平滑化
35
ゲート
乱数出力
乱数性判定
アラーム
40
41

【図２】


6.3 V
0 V
(a) ツェナーダイオードからの雑音
(b) 増幅された雑音
(c) 雑音の交流成分
1 1 0 1
0 V
サンプリング点
サンプリング点
(d) ランダムな矩形波
(e) 0,1の真性乱数の系列

【図３】


乱数性判別ルーチン
S1
乱数データ取込
S2
各乱数データの出現確率は一様か？
Y
N
S5
各乱数データ値は非同期的か？
S6
各乱数データ値は非系列的か？
S3
ゲートオフ出力
S7
ゲートオン出力
アラーム出力
S4
リターン